INFORMATION SECURITY and IT RISK MANAGEMENT

Manish Agrawal
Alex Campoe
Eric Pierce

WILEY

Information Security and IT Risk Management

Manish Agrawal, Ph.D.
Associate Professor
Information Systems and Decision Sciences
University of South Florida

Alex Campoe, CISSP
Director, Information Security
University of South Florida

Eric Pierce
Associate Director, Information Security
University of South Florida

WILEY

Vice President and Executive Publisher	Don Fowley
Executive Editor	Beth Lang Golub
Editorial Assistant	Jayne Ziemba
Photo Editor	Ericka Millbrand
Associate Production Manager	Joyce Poh
Cover Designer	Kenji Ngieng

This book was set by MPS Limited.

Founded in 1807, John Wiley & Sons, Inc. has been a valued source of knowledge and understanding for more than 200 years, helping people around the world meet their needs and fulfill their aspirations. Our company is built on a foundation of principles that include responsibility to the communities we serve and where we live and work. In 2008, we launched a Corporate Citizenship Initiative, a global effort to address the environmental, social, economic, and ethical challenges we face in our business. Among the issues we are addressing are carbon impact, paper specifications and procurement, ethical conduct within our business and among our vendors, and community and charitable support. For more information, please visit our website: www.wiley.com/go/citizenship.

ISBN 978-1-118-33589-5 (paperback)

10 9 8 7 6 5 4 3 2

List of Figures

Preface

Unlike the problem facing the Superb Fairy-Wren (front cover), most information security problems we humans face are not matters of life and death (for more on the Wren's problem, please see the critical thinking question in chapter 9). However, they are vexing, expensive and frequent enough to make information security a contemporary profession and the topic of information security a worthwhile subject to study.

This book is designed to serve as the textbook for a one-semester course devoted to information security. It is focused on helping students acquired the skills sought in the professional workforce.

We start by introducing the professional environment of information security. After the student is convinced of the merits of the subject, the book introduces the basic model of information security consisting of assets, vulnerabilities, threats and controls. The rest of the course is devoted to characterizing assets, vulnerabilities and threats and responding to them using security controls. The book ends by integrating all these topics within the general umbrella of organizational risk management. At the end of the course, students should have an awareness of how information security concerns have evolved in our society and how they can use contemporary frameworks to respond to these concerns in a professional environment.

The book comes with a full set of end-of-chapter exercises. There are five kinds of exercises at the end of every chapter:

1. Traditional end-of-chapter questions are designed to improve student understanding and recall of common topics in information security.
2. An example case at the end of each chapter allows students to apply the knowledge in the chapter to business contexts.
3. There is a threaded design case running through all the chapters in the book. In this case, students play the role of the Chief Information Security officer of a typical state university and are confronted with situations related to the topics discussed in the chapter. They are required to analyze and evaluate the situation in light of the knowledge in the chapter to create a solution that addresses the present problem.
4. A critical thinking exercise introduces students to analogous situations and relate the ideas from the chapter to these situations. The problem confronting the Superb Fairy-Wren falls in this category.
5. Finally, each chapter has a detailed hands-on activity using a customized distribution of the CentOS Linux OS to be installed as a virtual machine using VirtualBox. We take great pride in this aspect of the book. We have carefully selected exercises that will help students become familiar not only with rudimentary information security tasks, but also with Linux systems administration. Eric in particular, has spent countless hours testing,

curating and maintaining the distribution. You may download the distribution from the textbook's companion website.

While the book is self-sufficient without the hands-on activity, this content is in direct response to employer demands and we do hope you will give your students the advantage of this aspect of the text. Chapters 2 and 3 introduce the basic setup and usage of the virtual machine. The instructions are detailed enough for students to be able to complete the exercises on their own.

When using the book, class time may be used in various ways. A traditional lecture format will work very well. Instructors interested in using class-time for more interactive activities will find that the end-of-chapter activities are a very useful way to use class time.

The author team integrates the different perspectives necessary to teach information security to an aspiring professional. Manish Agrawal is an MIS faculty member who designed this course and has taught it to MIS and Accounting students at the University of South Florida for over 5 years now. Alex Campoe is the Director of Information Security at the University of South Florida where he is at the frontline of the university's information security activities including incident response, policy development and compliance. Eric Pierce is responsible for identity management at the university. Many of the topics covered in the book are informed by their knowledge of the most important day-to-day activities that fall under the information security umbrella.

The Superb Fairy-Wren, though not strictly facing an information security problem, happens to use a solution that adopts many of the information security controls discussed in the text. The context also includes all the components of our basic information security model – assets in the form of the life of offspring, vulnerabilities in the form of delayed hatching, threats in the form of parasitic birds and controls including passwords. We think it succinctly describes the text.

We are eager to hear any comments you may have about the book – suggestions for improvement, errors and omissions, bugs in the virtual machine, and any other issues you may encounter. We will do our best to respond directly to you with corrections, and also address them as errata to be published on the textbook companion site. We obviously would also like to hear complementary things if the book helped improve your understanding of the subject, improved your teaching, helped you land a job, or helped you on the job. Those comments can give us indications on how to strengthen future editions of the book. Comments may be sent to the first author at magrawal@usf.edu.

Table of Contents